начали резко увеличиваться в определенном моменте. Во-вторых, так же основываясь на данных таблицы 2, было выявлено, что показания датчика зависят от температуры окружающей среды.

Обработав данные таблицы 2, было выведено уравнение зависимости:

$$y(x) = 4*10-23*x11.018, \quad (1)$$

где y(x) – корректный выходной сигнал датчика MQ 9; x – значение, считываемое с датчика угарного газа MQ 9.

Таким образом, в рамках поставленной задачи была выполнена аппаратная и программная часть работы, а так же была произведена калибровка датчика угарного газа MQ-9 в лабораторных условиях. Из проведенной работы можно сделать вывод, что данный программно-аппаратный комплекс не подходит для обычного измерения концентрации газа и его можно использовать только для обнаружения пороговой концентрации угарного газа в атмосфере.

Список использованных источников

1. Web-ресурс сети Интернет [сайт]. URL: https://ru.wikipedia.org. Статья "Arduino";
2. Web-ресурс сети Интернет [сайт]. URL:http://arduino.ru. Статья "Что такое Arduino";
3. Web-ресурс сети Интернет [сайт]. URL: http://autohome.org.ua/gas-sensor-mq9-detail. Статья «Датчик газа MQ-9»;

УДК 621.783.223.2

С. А. Бакланов, В. Ф. Ярчук

ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина», г. Екатеринбург, Россия

РЕАЛИЗАЦИЯ СМС-АВТОРИЗАЦИИ В СИСТЕМЕ

Аннотация

Доклад посвящен решению задачи реализации двухфакторной аутентификации пользователя в системе.

Ключевые слова: удостоверение личности, двухфакторная аутентификация, безопасность, сервис смс рассылок.

Abstract

The report is devoted to the solution of a problem of realization two-factor authentication in a system.

Keywords: credential, two-factor authentication, security, sms mailing service.

Двухфакторная аутентификация – это метод идентификации пользователя в каком-либо сервисе (как правило, в Интернете) при помощи запроса аутентификационных данных двух разных типов, что обеспечивает двухслойную, а значит, более эффективную защиту аккаунта от несанкционированного проникновения. На практике это обычно выглядит так: первый рубеж – это логин и пароль, второй – специальный код, приходящий по SMS или электронной почте. Реже второй «слой» защиты запрашивает специальный USB-ключ или биометрические данные пользователя. В общем, суть подхода очень проста: чтобы куда-то попасть, нужно дважды подтвердить тот факт, что вы м это вы, причем при помощи двух «ключей», одним из которых вы владеете, а другой держите в памяти.

На сегодняшний день двухфакторную аутентификацию можно рассматривать как один из самых надежных механизмов аутентификации. Метод двухфакторной аутентификации обладает еще одним важным преимуществом, которое заключается в способности предупреждать владельца аккаунта о попытке взлома: если на телефон или почту владельца аккаунта приходит сообщение с одноразовым кодом при том, что никаких попыток авторизации владелец аккаунта не предпринимал, такая ситуация указывает на попытку взлома — самое время менять оказавшийся ненадежным пароль!

Некоторые процедуры безопасности требуют трехфакторной аутентификации (3FA), которая обычно включает в себя владение физическим токеном и паролем, используемыми совместно с биометрическими данными, такими как отпечаток пальца или спектрограмма голоса.

В реальном мире злоумышленник может взломать защиту. Он может, например, найти карточку сотрудника и пароль в мусоре организации или небрежно выброшенное хранилище данных, содержащее базу паролей. Если же для аутентификации необходимы дополнительные факторы, злоумышленник столкнется, по крайней мере, с еще одним препятствием. Большинство атак происходит удаленно, через интернет. Двухфакторная аутентификация может сделать удаленные атаки гораздо менее опасными, потому что пароля недостаточно для доступа, и маловероятно, что злоумышленник также будет обладать физическим устройством, связанным с учетной записью пользователя. Каждый дополнительный фактор аутентификации делает систему более безопасной. Потому что факторы независимы друг от друга, и компрометация одного не приведет к неэффективности остальных.

Общая схема двухфакторной аутентификации показана на рисунке 1.

Рис. 1. Общая схема двухфакторной аутентификации

Для реализации смс авторизации в системе необходимо интегрировать в свое приложение сервис смс рассылок. Взаимодействие с сервисом осуществляется с помощью API, предоставляемого разработчиком сервиса. Для отправки смс необходимо передать на сервер сервиса смс рассылок некий объект (XML, JSON – это зависит от выбранного сервиса). Этот объект в общем случае содержит логин и пароль, необходимые для аутентификации в системе сервиса, текст сообщения и номер телефона, на который надо отправить это сообщение.

Документация по взаимодействию с API сервиса обычно предоставляется в личном кабинете пользователя сервиса смс рассылок после его регистрации.

Как это работает?

Вы на Ваш сайт помещаете форму, например, с 2 полями: поле для ввода номера абонента и поле для ввода одноразового пароля.

Абонент вводит номер телефона в соответствующее поле формы, Ваш сервер генерирует одноразовый пароль и выполняет Get-запрос на отправку этого пароля на введенный номер абонента.

Абонент получает пароль и небольшой текстовой инструкцией в СМС. Например, "Пароль для входа на сайт www.yourdomain.ru - 1234".

Абонент получает СМС-сообщение с одноразовым паролем и вводит его в соответствующее поле формы.

Ваш сервер сверяет введенный пароль с тем, что был сгенерирован, и дает зайти на сайт/зарегистрироваться или выдает ошибку с просьбой ввести пароль еще раз.

Как реализовать?

Для написания приложения используем платформу ASP.NET MVC. Отправлять объекты на сервер смс рассылок будем по протоколу HTTP. В C# для этого используется объект HttpWebRequest.

При входе на наш сайт пользователь попадет на форму авторизации. Если пользователь не зарегистрирован в системе, ему предлагается зарегистрироваться. При этом пользователь вводит логин, пароль, номер телефона. Эти данные сохраняются в базе данных. Пароли хранятся в виде хэша.

Пользователь хочет авторизоваться. Он вводит логин, пароль и запрашивает код. При этом на сервере срабатывает метод SendSmS(). Этот метод принимает значение, введенное пользователем в поле «Логин». Если такой пользователь существует, то на его номер отправляется смс с кодом.

Помимо того, что код отправляется пользователю по смс, он шифруется при помощи хэш-функции и хэшкод записывается в куки. Кукисы – это часть информации, отсылаемая сервером браузеру, которую браузер возвращает обратно серверу вместе с практически каждым запросом.

Вместе с ответом на запрос кода, пользователю приходят куки следующего вида [sms_cookie = hashcode]. Время жизни куки установлено 15 минут. Получив смс с кодом, пользователь вводит код в поле формы авторизации. Когда пользователь пробует авторизоваться на сервер приходит:

– логин;

– пароль;

– код;

– куки (хэш кода).

К коду, отправленному пользователем, применяется та же хэш-функция, и полученная строка сравнивается со строкой из куки. Пароль сравнивается с паролем из базы данных. Таким образом, проверяются два фактора – пароль, код. В случае совпадения, пользователь успешно авторизуется в системе.